Cynthia E. Ayers

Cynthia Ayers is a national security threat analyst, currently working as an independent consultant within the Mission Command and Cyber Division of the Center for Strategic Leadership, U.S. Army War College. Ms. Ayers retired from the National Security Agency (NSA) in 2011 with over 38 years of government service. Her intelligence community career included a position as NSA Representative to the DCI's Counterterrorism Center at CIA headquarters, where she worked throughout the attack on the USS *Cole* and the 9/11 crisis (2000-2002). Her government service culminated in an eight-year assignment as the National Security Agency's Visiting Professor to the U.S. Army War College (USAWC), where she taught electives on cyberwarfare, contemporary threats to national security from an intelligence perspective, and military applications of artificial intelligence. She advised students on research concerning strategic intelligence, counterterrorism, cyber warfare, the Middle East, and critical infrastructure protection.

Post-retirement, Ms. Ayers was employed as Vice President of EMPact America, a bipartisan, not-for-profit group working in support of electric grid vulnerability mitigation. She was later asked to be involved in a congressionally-sponsored task force looking at critical infrastructure issues, and is now Deputy to the Executive Director of the Task Force on National and Homeland Security. In that capacity, she recently testified before the Canadian Standing Senate Committee on National Security and Defence.

Ms. Ayers has written several published articles on national security issues, a book chapter on the cyber threat to critical electric infrastructure, and co-authored academic papers on the development of cognitive agents for intelligence analysis.

TESTIMONY OF

CYNTHIA E. AYERS,
DEPUTY TO THE EXECUTIVE DIRECTOR
TASK FORCE ON NATIONAL AND HOMELAND SECURITY

BEFORE THE

ENERGY POLICY COMMITTEE,
MICHIGAN HOUSE OF REPRESENTATIVES

on
March 7, 2017

Note: The views expressed in this product are those of the author and the Task Force on National and Homeland Security, and do not necessarily reflect the official policy or position of the U.S. Army War College or any Intelligence Agency within the United States Government.

The Cyber/Smart Grid Tech Threat to the Integrated North American Critical Electric Infrastructure

Honorable Chairman Glenn and Distinguished Representatives –

Thank you for this opportunity to discuss a topic that I believe is of primary importance to the security of the people of Michigan and the entire United States.

I am a threat/warning analyst with 44 years of experience, mostly as an employee of the National Security Agency (NSA), at times attached to other organizations to include:

- the Central Intelligence Agency's Counterterrorism Center during the attacks on the USS Cole and 9/11, as well as
- the U.S. Army War College (USAWC) where, for 8 ½ years as the NSA Visiting Professor, I taught Cyberwarfare, Current Strategic Threats to National Security, and Military Applications of Artificial Intelligence. I am currently employed at the USAWC as a strategic cyberwarfare consultant.

It is also my honor to serve as Deputy to the Executive Director of the Congressionally-sponsored Task Force on National and Homeland Security, as well as on the advisory board of Canada's Mackenzie Institute.

My testimony will concentrate on the possibility of a catastrophic cyber attack to the systems we depend on for the delivery of electricity – the lifeblood of our modern civilization.

The Threat

In this modern, networked world, our country's strategic center of gravity ("the hub of all power and movement, on which everything depends"[1]) for both military and civilian sectors is the electric grid. Our critical electric infrastructure is therefore exactly where belligerents aim their weapons, both cyber and kinetic.

A successful military operation against an enemy's center of gravity will effectively remove that entity's ability to act or react, instantaneously and long-term. Such an attack against the electric grid of a country could easily win an entire war – and it can be done with relatively little effort as a strategic "first strike." Because a great deal of coordination is generally needed for a cyber-only endeavor of that magnitude, and cyber effects may not be long-lasting, it is probable that a first-strike option would begin with a major cyber distraction followed by a devastating kinetic blow to the strategic center of gravity – the grid.

Cyber threats to our electric infrastructure, from a variety of sources, have increased at an astounding rate. The aggregate attack statistics are overwhelming. For example, a small Midwestern utility consortium "recently detected nearly 4 million hacking attempts in one eight-week period."[2] But much like the growth of the Internet, the development of smart grid technology has been paramount, while security designed for components and networks remains deficient.

As our electric grid becomes "smarter" and more networked, it also becomes more vulnerable, making it a very inviting – perhaps *the most* inviting – target for adversaries. Threats specific to smart grid technology range from the tactical (e.g. house-to-house, building-to-building) to the national strategic level. As with cyber activities world-wide, operational attacks against small, inconspicuous elements (smart meters, for example) could ultimately have a much larger, truly catastrophic impact to the grid and to the society it sustains.

Smart Meters and Open Backdoors

Although security can always be improved, all networks, all systems – virtually anything computerized – can be hacked. As systems become more highly networked, it becomes easier for attackers to locate "backdoors." Multiple "smart" appliances and other home or business devices are being developed and sold on the market, with the assumption that IoT (Internet of Things) networking and metering will soon be (if not already) commonly available. Demand for full optimization of smart meters will ultimately rule out limited, billing-only usage (e.g. Meter

to Cash or M2C). The number of gaps in security will multiply per person, per household; and a successful ingress of any "backdoor" could have detrimental effects on neighbors, communities, regions, states, the nation and beyond (e.g. Canada and Mexico). Passive cyber defenses will be of prime importance, yet ubiquitous usage of large numbers of components will only serve to increase gaps in security, regardless of the options given to consumers.

Smart meters can provide digital backdoors to facilities (e.g. the home, office, building, etc.) via the items within (e.g. televisions, refrigerators, thermostats, etc.). They can also allow access to multiple components of external electric infrastructure.[3] Therefore, the use of smart meters must be carefully evaluated in the context of threats to personal safety as well as the safety of the grid.

Physical Security

A trip to Johns Hopkins Applied Physics Lab to speak with the young students who work on IoT networks will reveal the extent to which hackers can gain access to metered appliances, which – even individually – can reveal dynamic information such as whether a building is occupied, who the occupants are, and where they are located within the building. This information alone gives kidnappers, terrorists, or other types of attackers previously unimagined advantages.

Another physical safety aspect of smart meters was raised by a Fire Chief Duane Roddy during your hearing of February 21, 2017. In a discussion of electrical arching and a fire that began only 36 hours after the installation of a smart meter on his own home, the Chief stated that there is no surge protection associated with the new meters (older analog meters do have surge protection). It should be noted that massive surges (with much greater effects than weather related or other types of flow interruptions) are associated with severe space weather (geomagnetic storms caused by coronal mass ejections from the sun) and electromagnetic pulse (EMP) associated with high-altitude nuclear explosions – both of which have been known to cause arching and fires.[4]

Hackers are also figuring out how to cause surges, using smart meters to access air conditioning systems. "If an attacker were to turn the air conditioners on and off repeatedly, the [infiltrator] could create disturbances and imbalances in the grid that could trip breakers beyond the neighborhood they're targeting and cause an even more widespread blackout."[5]

Grid Security

Interestingly, hacker access to appliances within a networked building doesn't seem improbable these days; and the general idea of a need for increased grid security is gaining ground from public and private sector perspectives. "In a January 2016 poll, 84 percent of cybersecurity professionals believed there was a high or medium likelihood of a cybersecurity attack occurring this year that would be serious enough to disrupt critical U.S. infrastructure such as the electric grid."[6]

Nevertheless, it remains difficult to explain the potentially *lethal* aspect of adversarial intent in the cyber realm. We've grown used to so much inconvenience on the net, caused largely by hactivists and criminals, that thinking in terms of cyberwarfare (where cyber attacks may turn kinetic) is a difficult cognitive leap for some to make. It is, however, extremely important that all who are tasked with or otherwise concerned with the well-being of the grid understand the potentially devastating consequences of what has become the most plausible conflict scenario – a strategic cyber "first strike."

Strategic "First Strike"

Cyber analysts have relatively recently proposed that nations around the world are currently engaged in a "cyber cold war." If indeed that has been the case, the year 2015 might, in retrospect, be classified as the point at which the cyber cold war escalated to the very edge of a global "hot war." It began with revelations of system infiltration and data theft on a massive scale. It ended with a successful "show of force:" a message in the form of what could be considered a "proof-of-concept" display of a strategic cyber "first strike" strategy against an opponent's military and civilian center of gravity – the Ukrainian electric infrastructure.

The electric grid is a requirement, paramount for the continued functioning of modern society. Without it, there is no banking, no water sanitation, marginal health care, limited transportation, communications, food production, and (equally important) food distribution. Within a period of weeks to months without electricity, supplies of food, water, and medicines will be gone, and social order will spiral out of control. The result of a prolonged outage could ultimately be millions of deaths.[7] A successful "first strike" against an opponent's electric infrastructure could effectively – and possibly instantaneously – decide the outcome of a war.

The electric grid is the one essential element upon which all other critical infrastructures rely. Our adversaries (specifically Russia, China, Iran and North Korea) know this. They have written about it. They have warned us and threatened us. At least one actor – allegedly Russia – has now provided evidence of a cyber capability to disrupt civil society, with an operational component that portends full-scale war.

Proof-of-Concept

On December 23rd, 2015, "multiple regional power companies"[8] in Ukraine were identified as targets of a major cyber attack which resulted in a power outage to 225,000 customers (households, businesses, etc). A few months later, the United States Federal Bureau of Investigation (FBI) and Department of Homeland Security (DHS) convened briefing sessions across the U.S. for public utility asset owners, Industrial Control System (ICS) vendors, and government personnel, to deliberate the implications of the attack against the Ukraine's power infrastructure. These briefings represented a sea change, by both utilities and governing bodies, in public acknowledgement that cyber intrusions, previously believed to be merely benign (albeit with malicious intent), have evolved into dormant weapons that, when triggered, could be considered "acts of war."[9]

The cyber attack on the Ukrainian electric grid was a demonstration of power by the attackers. Although cyber and military conflict between Russia and Ukraine has been simmering since early 2014, this event was, in essence, a proof-of-concept for a larger application – a "first strike" that could neutralize and potentially destroy the center of gravity for virtually any opponent dependent on the continued availability of electricity. For Ukraine, this proof-of-concept was indeed an act of war. For the rest of the world, it was a message – an omen of what is yet to come.[10]

Dr. Adam Segal, writing for the Council on Foreign Relations, labeled a period beginning June 2012 as "Year Zero:"

- Cyber activities prior to Year Zero consisted mostly of espionage and criminal acts, as well as a continual low-to-mid-level digital clash among a wide variety of cyber actors.
- Events within Year Zero (to include the introduction of Stuxnet and Shamoon malware) proved that nation-states could, and would, inflict damage to the maximum

extent possible on public or privately owned targets, within their capabilities and means, in order to achieve their objectives.[11]

The question of whether the escalation evident with the Ukrainian grid attack is considered a "Year Zero" event is better left to analysts such as Dr. Segal. What is clear, is that objectives have expanded and intent has shifted. The victims of Stuxnet and Shamoon were computer systems. The main target of the 23 December cyber attack was the Ukrainian center of gravity. The end-users of the systems targeted were the citizens of Ukraine – their National Security depended upon electricity and their grid had been compromised.

No Longer Theoretical

The Ukrainian power outage, as the first (officially acknowledged)[12] successful cyber attack against a power grid, has "marked a major cybersecurity escalation global governments have long feared."[13] A digital "first strike," delivered remotely and stealthily as a devastating blow across the networks and against systems that are both critical to military operations and crucial to the maintenance of modern society, is no longer theoretical.

Based on analysis of the known operational aspects and malware associated with the event – a variant of BlackEnergy was identified as present – the Ukrainian attack is believed to have originated from within Russia. Originally intended for espionage, adaptations of BlackEnergy may now pose a threat to energy, water distribution and filtration, and financial systems worldwide.[14] In fact, similar attacks against a mining company and part of the national railway in Ukraine may have been part of the same attack scenario.[15]

This is the type of threat that American officials (to include former Defense Secretary Leon Panetta,[16] former DHS Secretary Janet Napolitano,[17] United States Cyber Command (USCYBERCOM) Commander and National Security Agency (NSA) Director Admiral Michael Rogers,[18] and the Director of National Intelligence (DNI) James Clapper[19]) have been warning the public about since 2012. It's interesting to note that the U.S. Industrial Control Systems Cyber Emergency Response Teams (ICS-CERT) have identified BlackEnergy malware within U.S. systems. Published warnings have surmised that the U.S. malware "campaign" may have begun as early as 2011.[20]

Arguably, the devastation resulting from a massive cyber attack may be more limited in scope than that expected of a high-altitude nuclear attack or a direct hit from a great geomagnetic

storm; but the abilities of attackers are growing as vulnerabilities lie unaddressed. Certainly, *at this point in time*, a more highly-coordinated effort would be necessary to initiate a continental-wide collapse and maintain it for a long period of time, but capabilities are ever-increasing and will undoubtedly remain relatively inexpensive to implement, with the additional benefit of limited or no attribution for the attackers. For example, KillDisk malware (seen in conjunction with BlackEnergy), which effectively "wipes" infected systems, adds to the disruption and can effectively limit attribution.[21] On-site spares could become difficult to maintain as "clean" replacements, due to the pervasive nature of systemic infections.

A U.S. team of cyber experts sent to Ukraine to investigate the event not only noted the physical damage caused by KillDisk malware associated with the attack, but also described actions associated with the monitoring of event response as well as continued disruptions intended to slow down the process of restoring power. The attackers were apparently performing surveillance, developing battle-damage assessments, and performing tactical maneuver in cyberspace, while adapting to conditions "on the ground." [22]

Peer and near-peer adversaries now have the resources to retain large numbers of cyber operators ("militias") to infiltrate, hide, conduct intelligence preparation of the battlespace, change data, disrupt system integrity, probe, prod, strike, and inflict damage conducive to further, incremental collapse[23] using valuable "zero-day" exploits.[24] Russia, China, Iran and North Korea are the main culprits at this level. Semi-state and non-state actors, such as those connected with the "so-called Islamic State,"[25] the hacktivist group Anonymous,[26] and the Syrian Electronic Army[27] are of somewhat lesser concern, although Ransomware attacks (which are gaining in popularity and sophistication) remain a threat to virtually all critical infrastructures.[28]

In testimony before the U.S. Senate Armed Services Committee on the 5th of April (2016), Admiral Rogers (in his capacity as Commander, USCYBERCOM), stated: "we have seen cyber actors from more than one nation exploring the networks of our nation's critical infrastructure—and can potentially return at a time of their choosing."[29]

Post Cyber Event Kinetic Attack

A cyber "first strike" to critical electric infrastructure could severely damage the military's ability to respond. Admiral Rogers warned that "if directed at the critical infrastructure that supports our nation's military, cyber attacks could hamper our forces, interfering with

deployments, command and control, and supply functions, in addition to the broader impact such events could have across our society."[30]

Furthermore, the distraction and disruption caused by an unexpected digital assault paves the way for post-cyber event kinetic action. In fact, the progress of digital "first strike" can be seen in the following aggressions involving Russia:

- "The first major cyber conflict" was in April of 2007,[31] when Russia expressed displeasure with the Estonian government over the movement of a World War II memorial in the capital city Tallinn. Estonia fell under cyber attack (mostly described as Distributed Denial of Service or DDOS) for a period of almost three weeks. (Moscow denied involvement.)
- In 2008, Russia used proxy cyber forces (or "third-party hackers") to assist with DDOS attacks against Georgia in order to disrupt communications prior to a Russian invasion. (Again, Moscow denied involvement with the cyber activities.) This was seen as a prototype for a "hybrid war."
- Cyber and military activities have been ongoing within Ukraine since early 2014, without yet reaching a climax associated with complete invasion, yet Ukrainian analysts believe there to be notable similarities between the "build-up" in the Ukraine and the earlier (pre-2008) conflict between Russia and Georgia.[32] The Ukrainian power outage ended within hours, and there was no reported military follow-on. The lack of action at the point of a grid-down scenario could, however, be explained as:
    - The intent to merely display capability and send a message; and/or
    - The need to obtain more information – in other words, the action was taken for the specific purpose of compiling intelligence on mitigation / recovery of data as "lessons learned" for a subsequent, larger effort.

The possibility of a cyber "first strike" against the electric infrastructure of a much larger opponent may not be far off. The use of cyber weapons for the purpose of power disruption does not rule out subsequent attack with weapons that have lasting effects (e.g. a high-altitude nuclear device). In fact, there are benefits to the utilization of cyber weapons for a "first strike:"

- Flexibility with regard to operation initialization (e.g. "zero hour");
- The ability to use the same deployed cyber weapon for intelligence surveillance and weapons activation, as well as other functions;
- The ability to monitor and modify deployed cyber weapons as deemed necessary;

- If deployment is successful, a cyber assault can mask (by virtue of data corruption or distraction) other activities associated with a conflict, to include the arrival of kinetic weapons, military forces, or pre-positioned proxy cells.

Passive Cyber Defense is not a Reliable Sole Defense

Industrial Control Systems and their Supervisory Control and Data Acquisition networks (ICS/SCADA) – essentially all computerized systems that attach to and/or interface with transmission and distribution equipment, whether or not they individually interface with the Internet – are highly vulnerable to attack. This is true of communications links and all equipment (transformers, generators, capacitors, etc) that could be manipulated, altered, denied access to, and otherwise damaged or destroyed via instructions from hackers and/or malware.

Malicious code can be introduced to the system via the internet, via wireless devices, and from external storage devices[33] (e.g. those used during system maintenance). There are a multitude of ways that malware can be injected into a system. Once system infiltration has been accomplished, equipment settings can be changed, effects can be modified, and attacks masked. The most widely known example is the Aurora generator test;[34] but the Stuxnet virus[35] brought major attention to the problem, as did the destruction of Aramco's 30,000 computers in August of 2012.[36]

In March of 2013, Trend Micro researcher Kyle Wilhoit released a report on his effort to discover the types and extent of cyber attacks on control systems. Having set up "honeypots" where hackers would believe that they were able to control "fake gauges" of a water plant, Wilhoit found a surprising number of attacks that were amazingly advanced and successful ("roughly 17 would have been considered 'catastrophic' to the water pressure pumping system" that was used as a honeypot). The attacks notably came from both international and domestic sources.

Protection against cyber attacks via usual methods (passive defense) is not enough to thwart major adversarial cyber operations. A 2013 Verizon report noted that "finding specific vulnerabilities and blocking specific exploits is a losing battle."[37] In a similar vein, Secretary of

Defense Panetta had earlier noted that the U.S. "won't succeed in preventing a cyberattack through improved [cyber] defenses alone."[38]

One reason that passive defense is not always the best defense is the time lag between attack and identification of attack-related activity, let alone the time needed to generate a software "fix." A major cyber intrusion and compromise of the US Army Corps of Engineers' National Inventory of Dams, attributed to Chinese military/government cyber actors in open source reporting, is one example that raised alarm over the possibility of a future cyber attack by China on the U.S. power grid.[39] The attacks occurred over a period of months, beginning in January (2013), only to be discovered in April – a delay that could be costly, if not deadly, in a cyberwar "first strike" scenario.

Passive defense is reactive and slow, as well as "patchy" in terms of efficiency. Because passive cyber defense will not always work, nor will it ever be enough, we need to look at other options for defense. An all-hazards approach is necessary to ensure protection of the grid.

Physical protections against electromagnetic pulse (EMP) and geomagnetic disturbance (GMD) will enhance protection against cyber attacks. Blocking devices and transient voltage surge suppression devices that are specifically designed to eliminate the threat from GMD and EMP effects will go a long way toward eliminating the cyber threat. This is because many cyber attacks utilize data manipulation to cause damage to transformers, generators, etc. Obviously, passive defense practices in the way of software upgrades, protection programs, and firewalls must not be discounted; but they need to be supplemented by physical mitigation measures.

Risk Management Practices and Grid Security Are Not Compatible

"Worst case" does happen. In war, strategies designed to successfully employ worst case scenarios against an enemy are intentional. "Experienced practitioners . . . aim to identify the enemy's center of gravity and its critical vulnerabilities, then concentrate superior combat power to exploit those critical vulnerabilities, thereby forcing the enemy's culmination and so achieve decisive success."[40]

Consider the possibility that in one decisive action, critical vulnerabilities existing within our electric infrastructure could be exploited so successfully ***that the first and last battle in the next war occur simultaneously.***

In 2013, in response to a recent Executive Order (*Improving Critical Infrastructure Cybersecurity*[41]), a Brookings paper entitled *Bound to Fail: Why Cyber Security Risk Cannot Simply be 'Managed' Away*, was published. As the title would suggest, the authors criticized the Executive Order as insufficient because of its reliance on risk management and voluntary participation. ***"Business logic," which the authors note as inherent in the risk management framework, "ultimately gives the private sector every reason to argue the always hypothetical risk away, rather than solving the factual problem of insanely vulnerable cyber systems that control the nation's most critical installations*** **[italics added]."**[42]
Indeed, this has been the experience of those who have taken stances on grid protection against other types of attacks (e.g. high-altitude nuclear and radio frequency weapons) and natural disasters (e.g. great geo-magnetic storms caused by coronal mass ejections).[43] The North American Electric Reliability Corporation (NERC) is specifically cited by Langner and Pederson in the Brookings report as having difficulties with critical infrastructure protection (CIP) standards with regard to cyber security.

Risk-based models, as noted by the Brookings study,[44] effectively cause the user to ignore the outliers and engage only in the "most likely" threat. The complete, unquestioning acceptance of such has led us to a point where "worst case" is dismissed as "never going to happen," even when experience tells us otherwise. Our vulnerabilities are exposed by the over-reliance on risk management practices, and these vulnerabilities literally point our adversaries directly to the most effective strategic targets, tactics and procedures. While we, as nations, think "mutually assured destruction" (MAD) will keep catastrophic attacks from being attempted, our enemies think in terms of catastrophic first-strike scenarios to remove the United States and its neighbors as actors on the world stage – they know they can, because vulnerabilities are allowed to persist.

Reality

The Aramco attack (the Shamoon virus) in August of 2012 which destroyed over 30,000 computers was thought to be a counter-attack by Iran in retribution for the release of Stuxnet,[45] as were subsequent multiple and sustained attacks against U.S. banks. To the public's knowledge, little (if anything) was done in response. This has not yet seemed to have raised the ire of the grassroots. In fact, although Secretary of Defense Panetta raised the specter of a "Cyber Pearl Harbor" (as have others in the past), there is a great deal of published debate over the true capabilities of even the best cyber attackers. The discussion has led some to contend that a cyberwar would never cross the line into "physical space" or the kinetic realm,[46] in spite of the fact that operations associated with the 2008 Russian invasion of Georgia did just that.[47]

The substance of this open-source media debate on cyber capabilities is weakened by the fact that the public has not been made aware of the true extent to which actual cyber attacks have already been successful. The reasons for secrecy are myriad, and include not only classification of the data, but also an absolute need by business to exhibit trustworthiness as well as a fear of fallout related to insurance. (It may be a toss-up as to what business is more afraid of—cyber attacks, a loss of public confidence, or insurance "blowback.")

Cyber attacks, large or small, are most often thought of simply as excursions or provocations — without the kinetic attack/response assumptions associated with the event. Thus, to this point, even those resulting in substantial damage (e.g. leakage of classified data, loss of system functionality, or economic loss) – have not instigated a full-scale war, of either the cyber or kinetic varieties. Unless, that is, you count the current "cyber standoff" (multiple instances of cyber theft, vandalism, activism, intelligence gathering, and sabotage by a variety of actors)[48] as a type of long-term cold war enacted mainly by proxy.

Regardless, unpredictability in adversarial attack and response modes is something that must always be considered. There are occasionally unintended consequences of adversarial activities, especially if attacks have been sequential and cumulative. One such consequence is the possibility of a "trigger event" for a larger, less controlled cyber conflict leading up to full-scale kinetic war. The attack on the Ukrainian electric grid, as a proof-of-concept "first strike" weapon, may be the kind of cyber trigger that would initiate warfare in the other domains (Land, Sea, Air, and Space).

To the public's knowledge, however, there has been no definitive "red line" in regard to how much damage or loss a victim should accept before responding. It is to this point that a so-called "secret legal review," as reported by the *New York Times* (2013), speaks. The *Times* claimed that the President now "has the broad power to order a pre-emptive strike if the United States detects credible evidence of a major digital attack looming from abroad." The rules are said to be "highly classified."[49] This would seem to indicate concern of an adversarial catastrophic "first strike."

It has long been understood that one of the risks associated with initiating a cyber attack against a target is that the software involved can be turned around and used against the originator. Stuxnet, for instance, targeted a specific type and brand of industrial controllers which operated nuclear power plants in Iran. Although focused as an initial attack, once identified, nothing

prevented the malicious software from being revamped and redirected — making it more generic and/or focused on other types of systems.

It is advisable, of course, for the originator to harden vulnerable systems against blowback prior to unleashing damaging malware; but much depends on security classification, timing, and comprehensive identification of possible damage. Perhaps the well-publicized angst over attacks on U.S. critical infrastructure is indicative of a lack of adversarial intent on the part of the United States. Regardless, given the extent of the warnings issued since October of 2012, it seems that the United States is ill-prepared for a major attack against the electric grid. Such an attack, if well-coordinated as well as sufficiently staffed and resourced, could have catastrophic effects on the U.S. – and potentially the Canadian – population. If the grid were down for a year or more, over two-thirds of our population could be lost to malnutrition, disease, and chaos.[50] ***The "Pearl Harbor" analogy would be nowhere near sufficient to describe the extent of damage that would result.***

Furthermore, the analogy of a "Pearl Harbor event" could be short-sighted, by virtue of a subsequent lack of capability to respond. This would most probably be the intended result of any attack scenario against a bigger, more militarily equipped enemy, especially if a power grid attack had been previously and publicly cited as one of the few "trigger events" that would be considered an "act of war." It should be noted that Panetta's description was essentially that – "if a cyber attack . . . crippled our power grid in this country, took down our financial systems, took down our government systems, that would constitute an act of war."[51]

The Congressional EMP commission report on critical infrastructure stressed that everything (including banking and government) hinges on the success or failure of the power grid.[52] If the U.S. is ever hit with a catastrophic, long-term "grid-down" scenario, no matter what the exact cause, any response might be too late (and therefore irrelevant) for those within the affected area. ***It's hard to consider how to respond to a "cyber trigger" that is, in itself, a "civilization-ending event."***

If, as the *Times* reported, a pre-emptive authority has been given to the President, it is no doubt due to an understanding that ***we have yet to see "worst case."*** Those who prefer to advise the government to wait until "a safety issue is pervasive"[53] or until evidence of the effects present themselves *en masse*,[54] may not be expecting a "worst case" trigger event – a catastrophic attack against our center of gravity.

Why the Rush?

If recent history is any example, the North American Electric Reliability Corporation could take 10 to 15 years (or longer) to adopt standards necessary for an all-hazards approach to mitigation. By then, it could (and probably will) be too late. Our adversaries are "at the door," knowing that we are currently vulnerable. Some have already threatened use of high-altitude nuclear EMP attacks, others are building weapons to ensure catastrophic grid collapse, and still others have been attacking us incrementally within the cyber realm. They have more recently displayed the capability of a "first strike" against a nation's electric grid.

A continental crisis is already upon us, in the form of an extremely vulnerable power generation and distribution system existing within an increasingly threatening environment. As a threat/warning analyst with over 40 years of experience working national security issues, I regard the potential loss of our country's electric infrastructure as the number one threat we currently face. The facts have been presented in a number of reports – they speak for themselves.

Due to the manner in which cyber attacks are propagated, cybersecurity is everyone's business. It is ultimately up to individuals and the companies who employee them, to do what is necessary to meet this looming crisis. Leaders, in both the public and private spheres, must provide an environment conducive to the preservation of national security. The destruction of our critical infrastructure is not simply a "worst case scenario" that will probably never happen. It is a "weapon of choice" that will ensure victory to the attacker.

Our enemies are already protected against critical infrastructure collapse. We cannot and must not wait to protect our own center of gravity against inevitable attack.

ANNEX

Recommendations:

- Use an "all-hazards" approach for grid mitigation. **Retain analog systems to the extent possible.**
- Remove barriers to (or incentivize) cyber event reporting. Refrain from "punishing" utilities for reporting cyber intrusions or other grid deficiencies. Punishment (with or without fines) encourages a lack of reporting.[55]
- Establish clarity of authorities, roles, and responsibilities.[56]
- Maintain training standards that include the potential for manual operations (if possible) as well as constant questioning of data displayed (corruption/manipulation of data has been noted in cyberattacks).[57]
- Utilize best cybersecurity practices. ICS-CERT has posted Department of Homeland Security, Department of Justice, and National Security Agency document entitled *Seven Steps to Effectively Defend Industrial Control Systems.* Contact information for all three organizations is included.[58] (See: https://ics-cert.us-cert.gov/Seven-Steps-Effectively-Defend-Industrial-Control-Systems)
- Retain "clean" and/or analog spares (e.g. uninfected control systems) and other resources to the extent possible.
- Secure and maintain all physical grid components, as damage can be exacerbated and amplified by weak links, even if the initiation of an event is cyber specific.[59]
- Do not depend on risk management for any aspect of grid security.[60]

Endnotes

[1] Strange, Joe and Iron, Richard (n.d.). "Understanding Centers of Gravity and Critical Vulnerabilities," http://www.au.af.mil/au/awc/awcgate/usmc/cog1.pdf (accessed March 5, 2017).
[2] Begos, Kevin (2016, November 11). *Protecting the Power Grid.* CQPress http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016111100 (accessed March 5, 2017).
[3] Downing, Louise and Polson Jim (2014, July 2). "Hackers Find Open Back Door to Power Grid With Renewables," *Bloomberg*.
[4] Foster, J. S. Jr.; Gjelde, E; Graham, W. R.; Hermann, R. J.; Kluepfel, H. M.; Lawson, R. L.; Soper, G. K.; Wood, L. L. Jr.; and Woodard, J. B. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures,* Washington, DC;
[5] Zetter, Kim (2016, February 9). "How to Hack the Power Grid Through Home Air Conditionings," Wired https://www.wired.com/2016/02/how-to-hack-the-power-grid-through-home-air-conditioners/ (accessed March 5, 2017).
[6] Begos, Kevin (2016, November 11). *Protecting the Power Grid.* CQPress http://library.cqpress.com/cqresearcher/document.php?id=cqresrre2016111100 (accessed March 5, 2017).
[7] Foster, J. S. Jr.; Gjelde, E; Graham, W. R.; Hermann, R. J.; Kluepfel, H. M.; Lawson, R. L.; Soper, G. K.; Wood, L. L. Jr.; and Woodard, J. B. (2008, April). *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack: Critical National Infrastructures,* Washington, DC;
[8] Radiflow (2016, January 21). "The Ukrainian Outage," *Radiflow*.
[9] Tapper, Jake (2012, May 27). "Leon Panetta: A Crippling Cyber Attack Would be 'Act of War," *ABC News*.
[10] Defazio, Congressman Peter (2016, April 14). *Blackout! Are We Prepared to Manager the Aftermath of a Cyber-Attack or Other Failure of the Electrical Grid?* U.S. House of Representatives Committee on Transportation and Infrastructure.
AFP (2016, March 2). "NSA Chief Worries About Cyber Attack on US Infrastructure," *Security Week*.
[11] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 1-16.
[12] See Harris, Shane (2014). *@War: The Rise of the Military-Internet Complex*. New York: Houghton Mifflin Harcourt. See also Brenner Joel (2011). *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*. New York: The Penguin Press, p. 105 for reports of apparently successful grid attacks against other nations.
[13] Tomkiw, Lydia. (2016, January 6). "Did Russia Kill Ukraine's Electricity? Cyberattack Linked to Power Outage Has Global Implications," *International Business Times*.
[14] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 13; See also, ICS-CERT Alert (ICS-ALERT-14-281-01E), (2016, March 2). *Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*.
[15] Wilhoit, Kyle (2016, February 11). "KillDisk and BlackEnergy Are Not Just Energy Sector Threats," *Trendlabs Security Intelligence Blog*. TrendMicro.
[16] Bumiller, Elisabeth and Shanker, Thom (2012, October 11). "Panetta Warns of Dire Threat of Cyberattack on U.S.," *The New York Times*.
[17] Levine, Mike (2013, August 27). "Outgoing DHS Secretary Janet Napolitano Warns of 'Serious' Cyber Attack, Unprecedented Natural Disaster," *ABC News*.
[18] Lyngaas, Sean (2014, November 20). "NSA Director Predicts Major Cyberattack by 2025," *FCW*.
[19] Gertz, Bill (2015, September 16). "DNI: Russians Hacked U.S. Industrial Control Nets," *The Washington Free Beacon*.
[20] ICS-CERT Alert (ICS-ALERT-14-281-01E), (2016, March 2). *Ongoing Sophisticated Malware Campaign Compromising ICS (Update E)*.
[21] Tucker, Patrick (2016, March 9). "The Ukrainian Blackout and the Future of War," *Defense One*.
[22] Abdollah, Tami (2016, February 27). "Sophisticated Attackers Hacked Ukrainian Electric Grid," *Military.com*; See also Gertz, Bill (2016, March 9). "CYBERCOM Says Cyberattacks on Infrastructure Coming," *The Washington Tiimes*.
[23] Burke, Garrance and Fahey, Jonathan (2015, December 22). "Iranian Hackers Breached US Power Grid to Engineer Blackouts: Investigation Finds Outdated Cyberdefense for America's Key Infrastructure, With Attackers Lurking, Waiting to Strike," *The Times of Israel*. See also: Clayton, Mark (2013, February 27). "Cyberattack Leaves Natural Gas Pipelines Vulnerable to Sabotage," *Christian Science Monitor*.

[24] Tucker, Patrick, (2016, March 9). "The Ukrainian Blackout and the Future of War," *Defense One*. For more on "Zero Day exploits," see Zetter, Kim (2014). *Countdown to Zero Day: Stuxnet and the Launch of the World's First Digital Weapon*. New York: Crown Publishers.
[25] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[26] Liebowitz, Matt (2012, February 21). Could Anonymous Really Knock Out the Power Grid? *NBC News*.
[27] Department of Justice (2016, March 22). *Computer Hacking Conspiracy Charges Unsealed Against Members of Syrian Electronic Army*. Washington, DC: Department of Justice Office of Public Affairs.
[28] Storm, Darlene (2016, January 27). "No, Israel's Power Grid Wasn't Hacked, but Ransomware Hit Israel's Electric Authority," *Computer World*.
[29] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[30] Rogers, Admiral Michael S. (2016, April 5). *Statement Before the Senate Armed Services Committee*. Washington, DC: U.S. Senate.
[31] Segal, Adam (2016). *The Hacked World Order*, New York: Council on Foreign Relations, p. 60-66.
[32] Euromaidan Press (2015, September 5). Kremlin Hybrid War Tactics in Georgia, 2008, and Ukraine, 2014-2015: Different Countries, Same Playbook. Euromaidan Press.
[33] ICS-CERT (2012). Industrial Control Systems Cyber Emergency Response Team Monthly Monitor (ICS-MM201210) October/November/December 2012: http://ics-cert.us-cert.gov/monitors/ICS-MM201210 (accessed 30 September 2013).
[34] Burkhart, Lori A. (2008, January), "Cyber Attack! – Lessons Learned: Aurora Attack," *Fortnightly Magazine*.
[35] Kushner, David (2013, February 26). "The Real Story of Stuxnet: How Kapersky Lab tracked down the malware that stymied Iran's nuclear fuel enrichment program," *IEEE Spectrum*.
[36] Infosecurity Magazine (2012, August 24) "Shamoon likely the malware used against Saudi oil giant Aramco," *Infosecurity Magazine*.
[37] Chuvakin, Anton (2013, April 29) "Verizon DBIR 2013 Highlights and Favorites;" Verizon (2013) *2013 Data Breach Investigations Report*.
[38] Bumiller and Shanker, "Panetta warns of Dire Threat of Cyberattack on U.S."
[39] ICS-CERT (2013). Industrial Control Systems Cyber Emergency Response Team Monthly Monitor (ICS-MM201306) April/May/June 2013: http://ics-cert.us-cert.gov/monitors/ICS-MM201306 (accessed September 30, 2013).
[40] Strange, Joe and Iron, Colonel Richard (n.d.). "Part 2: *The CG-CC-CR-CV Construct: A Useful Tool to Understand and Analyze the Relationship between Centers of Gravity and their Critical Vulnerabilities."*
[41] Obama, President Barak H. (2013, February 12) *Executive Order: Improving Critical Infrastructure Cybersecurity*.
[42] Langner, Ralph and Pederson, P. (2013, February) "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away," February 2013, *Center for 21st Century Security and Intelligence*.
[43] Kappenman, John. G. (2012, April 30) *Prepared Testimony of John G. Kappenman Before the U.S. Federal Energy Regulatory Commission Technical Conference on Geomagnetic Disturbances on the Bulk Power System*; and Pry, Peter Vincent (2012, April 30) *Testimony of Dr. Peter Vincent Pry, Executive Director, Task Force on National and Homeland Security, Before the U.S. Federal Energy Regulatory Commission Technical Conference on Geomagnetic Disturbances to the Bulk Power System*.
[44] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."
[45] Shanker, Thom and Sanger, David E. (2012, October 13) "U.S. Suspects Iran Was Behind a Wave of Cyberattacks," *The New York Times*.
[46] Clayton, Mark (2012, December 7) "'Cyber Pearl Harbor': Could future cyberattack really be that devastating?" *Christian Science Monitor*.
[47] Masters, Jonathan (2011, May 23) "Confronting the Cyber Threat," *Council on Foreign Relations*.
[48] Ibid.
[49] Sanger, David. E. and Shanker, Thom (2013, February 3) "Broad Powers Seen for Obama in Cyberstrikes," *The New York Times*.
[50] Foster, et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*.
[51] Tapper, " Leon Panetta: A Crippling Cyber Attack Would Be 'Act of War.'"
[52] Foster, et al. *Report of the Commission to Assess the Threat to the United States from Electromagnetic Pulse (EMP) Attack*.

[53] Sternstein, Aliya (2013, February 1). "Carhacking," *Government Executive.*
[54] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."
[55] Brenner, *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare*, p. 106-107.
[56] Government Accountability Office (2016, April 4). *DOD Needs to Clarify Its Roles and Responsibilities for Defense Support to Civil Authorities During Cyber Incidents* (GAO-16-332). Washington, DC: U.S. Government Accountability Office.
[57] Tadjdeh, Yasmin (2013, July). "Cyberspies Can Destroy, Corrupt Data as Easily as They Snoop," *National Defense.*
[58] ICS-CERT (2015, December). *Seven Steps to Effectively Defend Industrial Control Systems.* Washington, DC: DHS, DOJ, NSA.
[59] Faza, Ayman, Sedigh, Sahra, and McMillin, Bruce (2010, April 21). "Integrated Cyber-Physical Fault Injection for Reliability Analysis of the Smart Grid," *Proceedings of the 4th Annual ISC Research Symposium*, Rolla, MO.
[60] Langner and Pederson, "Bound to Fail: Why Cyber Security Risk Cannot Simply Be 'Managed' Away."

Kevin Gawronski

From: Kathy Vosburg <kvosburg@sbcglobal.net>
Sent: Monday, March 6, 2017 10:13 PM
To: Kevin Gawronski
Subject: smart meters

Hi Kevin,
I saw an e-mail about smart meters with your contact information. Just thought I'd say hi.
My opinion about smart meters, should you want to know, is that it's advanced technology.
There's more data shared and more electromagnetic waves (radio frequency) generated through our cell phones.
So if the legislature is going to be concerned about our health, there are more onerous devises affecting us.
That's per my husband, the radio technician, now retired.

Kathy D. Vosburg
47395 Sugarbush Rd
Chesterfield MI 48047
Home: 586.949.3810
Fax: 586.949.9403

Kevin Gawronski

From: Mary Kabisch <seme3m@gmail.com>
Sent: Tuesday, March 7, 2017 1:02 PM
To: Kevin Gawronski
Subject: Utilities of choice bill number 4220

Dear energy policy committee, I have the right to choose what device is put on my house. Please pass this bill. Thank you for your time. Mary Kabisch

Sent from my iPhone

Kevin Gawronski

From: Ralph Stenman <restenman@sbcglobal.net>
Sent: Monday, March 6, 2017 3:33 PM
To: Kevin Gawronski
Subject: Fw: HOUSE BILL 4220.....NEEDS TO BE PASSED.....We need our Analog Meters!!!

We need our meter choice HB 4220 passed. This never should have happened to us or anyone. We will never recover the losses we endured being cut off with out notice on one of the hottest days of the summer.

To whom reads this,

We Ralph & Donna Stenman are 75 & 72 years of age.
We have medical letters from doctors, a cardiologist and primary care doctor, documenting that our health cannot tolerate smart meters.
We should have been eligible for a medical hold and able to keep our analog meters.

Having a smart meter on our home would cause a medical emergency.
Living without electricity, to avoid a smart meter causing a medical emergency, actually did cause a medical emergency as told below.
Either way, this is/was life threatening to us.

The shutoff Rules now being questioned in this case U-18098 are specific only to non-payment.
There is no mention of shutoffs due to smart meter - medical disputes.
No where in the Rule 133 Reporting Requirements is there a category to track smart meter - medical disputed shutoffs.
Neither the commission nor the legislature knows the true extent of all those now living without power because of smart meters nor the number forced to accept & pay for a non-analog meter opt-out for health reasons.

The Rules state that our power can be shutoff if we do not allow access to replace equipment.
Do not the Rules also state if you are not satisfied with the utilities actions you have the right to file a complaint, and your power cannot be shutoff. We did this and it changed nothing.
We are currently awaiting consideration from the U.S. Supreme Court.
DTE is well aware of this.

DTE still comes on to our property without permission to photograph our meter - to make sure we aren't stealing electricity.
I am on generator power as I type this.

The day of our shutoff

At 10:30 am on August 13, 2015 DTE Energy arrived at my home **WITHOUT NOTICE**. A van, one man, a black car and a lady dressed in black. Also along was Mr. Sikaska, Supervisor in a pink dress shirt. A little later one Farmington Hills Police car arrived he did not approach me or come to my door. I had been doing work in the house and was still in my bath robe, not dressed for the day yet. I had no idea they were coming, no notice, no letter, no nothing to help me prepare.

I went to my door and told them to leave my property this is not authorized. They ignored me and the man in the pink shirt continued up my drive way. I then went out my front door and told them they cannot do this, we are in the Court of Appeals. The meter man was at my meters and the lady in black was guarding him. When I got closer she blocked me from getting any closer. I told her you have no right to do this. The meter man went to his van for a wrench and went back to our meters as our meters are locked. I went back and told him to leave our meters alone. He laughed at me and thought it was a big joke. I told him this is not funny. Installing non ionizing radiation on people's homes that make them sick and you think it is funny? You should be ashamed of yourself....It was very upsetting to be so disregarded on my own property.

I could not find the paper work I wanted to show them on our court case....I was very upset, my blood pressure was way up and I was red as a beet. Afraid I might have a stroke. I called my husband who was at work. I was so very frantic and wanted him to come home. He told me to calm down, my blood pressure is up... and he left to come home.
The first to leave after standing on my neighbor's lawn talking was the meter man that drove the van and the man in the pink shirt Mr.Sikaukas and then the police. They were here about 45 minutes. They said nothing to me and just left the scene.

On August 14th, 2015 the next day.....The arrival of DTE Energy entourage..... 3 high lift trucks, couple vans, lots of people male and female all over my property and our neighbors lawns. Mr. McCormick, and 2 police cars. With two police officers that came to my front door. I was not dressed and had to ask if I could get dressed. They said yes. After getting dressed.....I went back to our meters and told them to leave them alone. It was chaotic, people everywhere, they were trying to take my safe Analog Meters off. I did not know who the lead person was so I asked him his name, he said Mr. McCormick...I said Mr. McCormick can you tell me why there are 3 families on my street, 2 of which we watched DTE Energy remove their smart meters and put back on Analog Meters...back in March of 2012...we have pictures, all meters are numbered, and easy to check. Why are you doing this to us....(pointing to his meter men trying to remove our Analog Meters) that were working perfectly. I also ask him why we can't have a choice? Wouldn't that be the fair thing to do, people are and have been getting sick with these meters. I believe Consumers Power is allowing choices.....the one Police officer was right there and heard me ask this question. He ignored my question.

After a few minutes he came around to the front and said something about the smart meter, I was so distraught and not hearing well, I was not sure what he said, I told him I could not consent to a smart meter on our home, and I wanted my husband to be here, he said you don't need your husband to be here.....and they cut my DTE electrical service off at the pole.....and left.....I was frantic, how could they do this.....We had no warning..... We had always heard the utility company **MUST PROVIDE ITS CLIENTS WITH A NOTICE TEN DAYS BEFORE SHUTTING OFF THEIR SERVICE.....AND A FIVE DAY RED FLAG NOTICE. Their excuse is: LOCKING OUR METERS IS A FIRE HAZARD TO NEIGHBORS WHILE THEY ARE INSTALLING SMART METERS ON HOMES AND THEN PUTTING LOCKS ON THEM. WHEN IN FACT THESE SMART METERS ARE**

THE FIRE HAZARD…….ANALOG METERS HAVE NEVER BEEN KNOWN TO BE A FIRE or HEALTH HAZARD. THAT SEEMS LIKE A CONTRADICTION TO ALL OF US. Not to mention the fact that Analog Meters have been stolen and to avoid that from happening we did put locks on them.

My husband then arrived home, we then had to go to a hotel as it was so hot that day and we were not doing well physically, or emotionally. So to get away we thought it would be a good idea to calm down and get our bearings. We stayed there for a week and then came back to our home. If it had a smart meter on our home we could not have done that as both Ralph and I have bad effects from the smart meter. I am a cancer survivor and they are a known cancer causer, a class 2b carcinogenic stated by the World Health Organization. So we began to live the best we could, the organic food in our refrigerator had to be thrown in the garbage… we had to purchase many items to help us survive in this horrible situation we were totally unprepared to be in……

In November it was getting cold out and we were having a hard time keeping our home warm. Ralph who had been in other wise good health came down with pneumonia and ended up in the hospital for 2.5 months with a collapsed lung, chest tubes and in the critical care unit.

Ralph came down with pneumonia approximately the week before Thanksgiving. He had been coughing a lot and running a fever, not feeling well. I took him to Urgent Care and they did a chest x-ray and saw that the pneumonia was extensive and sent him to the emergency room. I drove him by car. He was admitted at that time and on multiple antibiotics. He was in the hospital about a week....and wanted to come home for Thanksgiving.....they agreed reluctantly but he would have to be on oxygen.....He came home on oxygen the Wednesday before Thanksgiving... The oxygen required electricity. During this time our generator failed and the oxygen cut out ...he got worse and the Monday morning after Thanksgiving I had to take him to the Emergency Room as he was having difficulty breathing.....he was in congestive heart failure with severe pneumonia and admitted to the ICU unit.. .

His lung would not heal….there was great concern for his wellbeing. He was on a respirator for a while, and not doing very well….I thought I was going to lose my husband….they called in many specialists and he then did begin to heal after a special procedure to close his one lung, that needed to be done twice to help it begin to heal. Meanwhile our medical bills were beginning to grow.

In January he was able to go Rehabilitation for 2 months to learn to walk again, he lost approximately 50 pounds and was in a very weak condition…..after 2 months in Re-Hab he came home…..with Physical therapy at home 3 times a week. He suffered shortness of breath from the damage the pneumonia, and intensive care did to his lung…..he is unable to do much now. His recovery has been slow and bumpy…..but at least I have him back home. The last seven months have been almost unbearable. To say having our power shut off contributed to this…….I would be willing to say it did……the stress he endured was over whelming……and what I was put through was inhumane……

This viciousness shown by DTE is enough to shock the conscience of anyone needing electricity. We all are aware our electricity is a comfort and a security. We wrote DTE three letters on why we needed to keep our safe Analog Meter. We provided the courts with doctor letters from both of our doctors emphatically stating we could not live with a smart meter…….they were ignored.

All we want is our power turned back on, and to be able to keep our Analog Meter on our present home, with no additional cost, and compensation for the criminal act of being cut off without notice for reasons we could never consent. Our doctor letter and reasons for not wanting a smart meter (AMI Meter on our home were never disputed by DTE). We have to endure this horror story that still haunts us as we continue to live through the horrible, expensive DTE experience without any warning or notice given to help us to help us survive if that is possible…and the harm that has been done to us physically, and emotionally……and permanently to Ralph's health….is inhumane.

Thank you for reading our story.

Sincerely:
Ralph and Donna Stenman

Kevin Gawronski

From: Sue anne Demers <sueannedemers@gmail.com>
Sent: Monday, March 6, 2017 4:59 PM
To: Kevin Gawronski
Subject: HB 4220 Analog Choice (please fwd to each energy committee member-thank you)

Thank you for considering this HB4220 Analog Choice bill.

I absolutely, positively do not want this device on my home. I do not want it in the form of a gas, water or electric meter. I have a very small home and all of this wireless will impact me negatively. I have had other wireless devices impact me but these meters would be operating 24/7 and therefore no relief.These devices do not benefit me in any way and I should not be forced to have them. I would like to move to a larger home but cannot because I currently cannot take my analog meters with me.

It is rare that I am out and about in the daytime. I am constantly aware that DTE could come and replace my meter without warning. This has an economic impact on my community as well. When I am home I am not out spending money (stimulating the local economy). I am not out looking for a larger home and all the things that that home would need etc.

It is time that the citizens of Michigan have the assurance that we get to keep our safe analog meters for electric, water and gas. Please support HB4220 Analog Choice Bill so that people such as myself can get back to life as we knew it before these meters arrived.

Thank you,

Sueanne Demers

Kevin Gawronski

From:	Linda Harvey <bluemoonastrology@yahoo.com>
Sent:	Monday, March 6, 2017 5:11 PM
To:	Kevin Gawronski
Subject:	Hearing on HB 4220

Dear Clerk Gawronski: Please forward to every energy committee member. I apologize for sending this email last minute, but I had planned to attend in person, which is now not possible. Thank you, Linda Harvey

TO THE ENERGY COMMITTEE MEMBERS:

My name is Linda Harvey and I am writing to express my concerns, across the board , with Smart Meters and the "opt-out meters." DTE has run roughshod over citizens' rights by forcing Smart Meters or the opt-out meter on everyone without regard for the many problems and issues people are reporting. They deny, misrepresent, and cover up all complaints. It reminds us of the whole mishandling of the Flint water crisis. You know they are not doing this out of the goodness of their hearts as the expression goes, but only for what's in it for them. They are invading our privacy so they can increase the rates during the hours when we use our highest electricity. Areas in Canada and the United States were Smart Meters were first installed have all experienced hikes in utility rates.

For many, many years we had analog meters, which caused no problems in terms of safety, privacy, property owner rights, or health. Despite significant reporting of fires, especially in older homes, deep concerns about privacy, and documented reports of disturbing physical symptoms after the installation of either Smart Meters or opt-out meters (usually with the resident not even knowing that a change in the meter had occurred, thus it is impossible that it's "all in their heads"). Sick and elderly people have had their power turned off by DTE. They are really playing hardball in this matter and individual rights are suffering as a result.

Please vote for HB 4220. This is a GOOD bill and will restore choice to Michigan citizens about our privacy, our safety, and our health.

Thank you very much for time and consideration. Linda Harvey

Kevin Gawronski

From: Steve Tobey <swtobey@comcast.net>
Sent: Monday, March 6, 2017 5:40 PM
To: Kevin Gawronski
Subject: Public Statement Regarding HIB-4220

To Whom It May Concern,

I read the proposed HIB-4220 bill, and I would like to acknowledge my support for allowing customers to opt-out of the installation of smart meter technology by utilities. There are some concerns (notification, remediation, privacy, etc.) which I feel are adequately addressed. However, I feel the provision to charge customers up to $5/mo for not using smart meter technology is excessive. This is approximately equivalent to the monthly fee that cable companies charge for renting customers a cable modem or a digital tuner device. As an incremental add-on fee for having a person come to your house to read your analog electrical meter, which is the existing requirement, it seems more to be a punitive measure against those, who for whatever reason, choose to opt-out of the smart meter technology. The other troubling aspect of the bill is that the utility could classify all analog meter domestic use as occurring during peak, which has a higher KW/hr rate. There is precedence for this view because that is what happened in CA when smart meters were installed, and the utilities started billing customers for peak utilization rates.

Regarding the use of smart meter technology, part of the difficulty with achieving scientific consensus on non-ionizing radiation (NIR) is that it is only examined from two perspectives: thermal heating [mW/g] and current induction [mA/mm]. Neither of these gross measurement techniques accounts for subtle effects on cell morphology, biochemistry or the long-term neurological/physiological effects. Health Canada recently revised its Safety Regulations on exposure to NIR, and there is an increasing body of evidence that even these limits are too permissive. Unfortunately, as some of the public is already aware of, there is a corporate conspiracy to suppress this type of information because of its financial impact on currently widely deployed technologies that use NIR. If the committee is interested in a comprehensive listing of NIR currently used in medical devices with an extensive reference section, it can be downloaded from www.icnirp.org.
[www.icnirp.org/cms/upload/publications/ICNIRPDiagnostic_2017.pdf]

The 2015 revisions to Health Canada NIR Safety Regulations were based on scientific research released in 2009. The ICNIRP working group responsible for the research is in the process of revising their recommendations again, making them even more restrictive. I point this out because it took six years for Canada to take definitive action. Things here in the USA are considerably more retarded. The current administration and U.S. Congress are taking a dismissive stance on the use of scientific evidence, which makes anything positive happening even more remote. I feel it is vitally important to understand and acknowledge the concerns of the public. All things having to do with radiation involve; source strength, shielding, physical displacement, and exposure duration. It is a tragedy that the scientists who are trying to protect us have such a hard time convincing corporations and our government to do the right thing.

Respectfully Submitted,

Stephen Winter Tobey, Jr.
2496 Colony Way
Ypsilanti, MI 48197

Pamela B. Wallace
168 Cloverport Ave.
Rochester Hills, MI.
48307

Monday March 6, 2017

House Energy Committee,

I am writing to ask for your support for HB 4220 and analog utility metering choice here in Michigan. For me an option of a mechanical analog meter is absolutely essential. I am a part of the population that is sensitive to electronic devises and my body is not able to physically tolerate a smart/advanced or current opt-out meter on my home or business. When overly exposed, I have ongoing physical symptoms that get in the way of my daily life. My physician has substantiated this for DTE on numerous occasions. Also record of my physician's statement can be found in the record of the House Oversight committee hearing from December 2014.

Because of my circumstances, I began reaching out to DTE over 5 years ago to let them know of my situation and to request an accommodation and the ability to retain the use of my analog mechanical meter. Originally the company assured me that I would be able to be noted as "refused" with regards to the smart meter or any meter upgrades and that I could retain use of my analog meter. My "refusal" reference case number was: #100140472.

As time progressed DTE's position changed without warning and I began getting notifications from the company stating I would have to replace my analog meter. Progressively the notification became more threatening even going so far as to threaten to put a smart meter on our home when we were not at home. When I approached the company regarding this, I began to get completely different and contradicting information from the different representative I spoke with about my personal situation and the advanced metering program in general. I was told on more than one occasion that someone in the company may have "dropped the ball" with regards to my information or that the 'right hand doesn't always know what the left hand is doing around here." I became concerned and began requesting more specific and clarifying information on my health issues, possible accommodations, answers to safety questions, etc. from the company and the leaders of the advanced metering program. I also requested a reconciliation process, none of which to date have ever been addressed or provided.

After a year of not hearing from DTE, (my last conversation had been in October 2015 with Mrs. Ward, Mr. McCormick's assistant and things were left that Mr. McCormick would contact me if he needed me to do anything differently) this summer in July 2016,

DTE notified me while I was on vacation that I was on a shut off list. I was very surprised since I had heard nothing back from Mr. McCormick. I again requested to have the opportunity to discuss the medical circumstances of my case. DTE refused both my request and the request from Oakland Mediation Center who agreed to mediate for us. They also refused to wait until our return from vacation to resolve this matter and would not commit to not turning our power off while my family was away.

In these conversations, DTE told me that I had no other choice and that I would have to have a smart meter or an opt-out meter on my home. They told me that the MPSC had mandated them to replace all of the analog meters. When I called the MPSC to inquire about this, they told me that this was untrue and they had not mandated DTE to replace all of the analog meters. They said that DTE was a private company/ business and had complete control over what equipment they chose to use. They said they had no power over DTE and told me to go to my legislators for assistance.

Also during these conversations I relayed to both the MPSC and DTE that I would be willing to work with another electrical company that could accommodate my needs for an analog mechanical meter. Both told me that there was no other option for an energy provider in South Eastern Michigan. So this left me in the position of having to choose between my electricity, a necessary resource and my health and well-being.

Both the MPSC and DTE also shared that they would not be making medical accommodations with regards to the advanced metering program. I shared with them that this was a concern since they were making a medical determination on my case without ever reviewing my case and that their position, directly contrasted the medical opinion of my physician, who is licensed to practice medicine here in Michigan. Neither DTE nor the MPSC has anyone on staff with a license to make such a medical determination or to practice medicine in the state Michigan.

Another concern is while the company was not honoring my physician's diagnosis and letter (or from what I understand any medical letters that have anything to do with smart/advanced/opt-out meters and shut-offs) they are honoring physician letters that do not involve references to the advanced/smart meters in other medical hold shut off cases. This is highly discriminatory.

DTE did come and disconnected our power on November 29th 2016. They said it was due to the locking devise we had put on our meter box (which Michigan residents own and maintain) almost 3 years prior when they threatened to replace our analog meter when we were not home. They said a locked meter box was unsafe to our family and neighbors (my fire marshal and an electrical engineer said no.) I had told DTE many times that I would gladly take the lock of the meter box anytime should they ever need to service the meter. Due to the threats that they had made, I just wanted them to service the meter when we were home. When they came to disconnect on November 29th, I offered to take the lock off the meter box, I called the number they asked me to

from the letter they handed me, I accepted the opt-out meter (under duress) from Mrs. Howard (who said she was going to hang up on me because I asked her to tell the disconnect crew I had ordered and opt-out meter) and cooperated with everything they asked me to and they disconnected our power anyway. We were without power for over 30 hours. Very soon after the disconnect however they were out to remove my analog meter and replace it with an opt-out meter and to put their own two locks on my meter box (rep. Webber and Sen. Knowlenburg's offices contacted DTE about the safety/legality of their locking devise on our meter box, since they stated that the un-safety of locking devises were the reason for our disconnect, on November 30th and to date, they/we have still not received clarification on this matter from the company.)

And the day after the disconnect, I received another letter from DTE announcing their new smart meter program. They said they would be beginning to install smart meters in our area (they had installed all the smart meters in our area 3 years ago.) In their letter they also stated that I would have the choice between a smart or opt-out meter. A little more of the right hand doesn't know what the left hand is doing?

This is a very condensed version of the past 5 years. Honestly with regards to DTE it has ben extremely stressful for both my family and myself. Believe me, we never wanted to spend five years focusing on our electric meter, something we had hardly paid any attention to before. The facts I have stated within I have documentation for. Also the facts within are the precise reason that we need both your help with the utility and an analog choice option here in Michigan. This simple/easy solution thankfully solves it all. Please support/champion this bill – we truly need it.

Thank you and Most Sincerely,

Pamela Wallace

Joshuah Wallace
168 Cloverport Ave.
Rochester Hills, MI.
48307

Monday March 6, 2017

House Energy Committee,

I am writing to ask for your support for HB 4220 and mechanical analog utility metering choice here in Michigan.

As we move forward and have the benefits and the challenges that come with advances in our technology, we need to strike a very careful balance. It is very disconcerting to think that anyone, other than ourselves could have control over what level of technology we both utilize and have on our homes.

These are very personal decisions and people have many valid reasons for making the decisions they do regarding these matters. A utility cannot make informed and quality decisions on behalf of their customers in these areas and should not ever be in a position to.

Part of serving the public at the level that our utilities do here in Michigan, with a virtual monopoly, comes the responsibility of actually servicing the public, the whole public and their diverse needs. This is a very large responsibly and can be a lot for one company to successfully do. That is why there is a great deal of reason in having more than one company providing similar services/resources. They more effectively cover and represent our needs. Our utilities here in Michigan by being a virtual monopoly, have chosen to take on this enormous responsibility and will therefore need to provide the very high level of service to the community that goes with it.

There are many reasons that one might not be able to, or want to have a smart/advanced meter on their home and the utility needs to be able to provide for that. We are not asking for unreasonable, unfounded accommodations but a level of accommodation that is the norm and already present in companies and institutions that deal with the general public. This is absolutely to be expected and understood as part of the responsibly of the position.

An "our way or the highway approach" and refusal to hear/meanfully address and respond to customer concerns, is both unacceptable and irresponsible. Also a refusal to have only one part of the conversation, the part that supports your own views/position, leaving the rest out, is both uninformed and dangerous. The utilities in their handling of the roll out of advanced metering program, have steadfastly demonstrated their

inability/unwillingness to meet and/ or respond to customers concerns and basic needs. It is for this reason, that they need the supervision and the structure of law. This is especially essential given because they are only energy providers here in Michigan and we are not able to live without their resource. It seems we have seen some unskillful abuse of power and this cannot continue. In the two hearings held in the house on the smart meter, analog choice issue, hundreds of people have come out to be in attendance to express and attend to their concerns. This should inform us, as it is an indicator of the utilities current level of ability to handle their charge. At this point of the discussion, it is clear we need support from our legislator. HB 4220 is a fair bill that has room for everyone's needs, those who want smart meters, those who do not/cannot and those of the utility. Please support this bill.

Kevin Gawronski

From: Catherine Murau <MCMurau@msn.com>
Sent: Monday, March 6, 2017 7:29 PM
To: Kevin Gawronski
Subject: Yes on Utilities of Choice Bill 4220

Clerk Gawronski,

I am writing as a resident of the state of Michigan in favor of the Utilities of Choice Bill #4220. I oppose the mandatory installation of smart meters on our homes. Twenty-three other states have passed a law giving homeowners the legal right to choose if they want a smart meter on their home or not. Our state should stand up for the right to privacy of individuals, and for the right to choose on such a clear-cut issue.

Smart meters should not be forced on us without our consent. Please urge the Energy Policy Committee to bring this bill up for a vote in the House of Representatives. Please listen to the voices of individual citizens asking for basic rights.

Thank you and kind regards,
Catherine Murau
2010 Hall Avenue
Ann Arbor, Michigan 48104
734-834-7931

Kevin Gawronski

From: Patty McAllister <patty@dooilsnotdrugs.com>
Sent: Monday, March 6, 2017 8:46 PM
To: Kevin Gawronski
Subject: HR 4220

Dear Mr. Gawronski,

We are writing you today to urge you to support individual home owners to have free choice when it comes to the type of meter used on their homes for electrical usage. Individuals should have the right to choose whether or not they want to use this meter despite the potential health and privacy risks associated with them. It is bad enough that we cannot choose to get our electric service from another company, this is taking their monopoly another step further . Like many others, I am particularly sensitive to them and have experienced multiple issues since having the digital meter. We had to pay $67 initial fee and $10 monthly for a meter that is supposedly not transmitting yet is still causing issues. We should be able to get my analog meter back if we prefer and are able to submit our own reading monthly if necessary.

We strongly urge you to support this important bill.

Respectfully,

Anthony & Patricia McAllister
6260 Fordham Drive
Shelby Township, MI 48316

Kevin Gawronski

From: Colleen Satarino <collsata@gmail.com>
Sent: Monday, March 6, 2017 10:09 PM
To: Kevin Gawronski
Subject: Legislation regarding smart meters

I am a resident of Milan, Mi and I am contacting you to ask that you support Utilities of Choice Bill #4220 to allow Michigan residents to have the choice as to whether or not they want a smart meter. Over 20 other states have granted their citizens such rights and I hope the we will be granted the same rights in Michigan.

Colleen Satarino
9225 Mirage Lake Dr
Milan, Mi

Sent from my iPhone

Kevin Gawronski

From: M.J. Trosper <mjt48044@gmail.com>
Sent: Tuesday, March 7, 2017 12:00 AM
To: Kevin Gawronski
Subject: Comment for HB 4220 Hearing, March 7, 2017

To Chairman Gary Glenn and the House Energy Committee

I am writing to respectfully request that you vote to let HB 4220 move forward to the House floor. I fully support letting the residents of Michigan have a choice to keep their analog meter at no extra cost.

DTE's opt-out version is extortion. DTE has received millions of Federal dollars (actually, taxpayer money) to install their advanced meters (aka smart meters). In other words, DTE is using our money against us – forcing us to accept a device we do not need or want – for many reasons which have already been brought to your attention.

It is the duty of our elected representatives to protect the interests of their constituents over the wishes of the special interests. Please, support HB 4220 all the way!

Sincerely,
M. J. Trosper
Macomb

Kevin Gawronski

From: Kummerfb@aol.com
Sent: Tuesday, March 7, 2017 2:54 AM
To: Kevin Gawronski
Cc: kummerfb@aol.com
Subject: Support for HB4220

To: The House Energy Committee
c/o House Energy Committee Clerk: Kevin Gawronski

I strongly support House Bill 4220, which allows a utility customer to keep their mechanical/analog utility meters, opting out of the use of SMART meters or the like, without incurring punitive consequences. My wife and I have strongly objected that electric or any utility company or public service commission be allowed to mandate the use of such invasive metering systems, which violate privacy rights of consumers and allow monitoring of activities within the residence.

The concern for the health of some individuals increases the danger from SMART or similar meters from a privacy violation to a threat to health. My wife's doctor has signed a letter indicating the added danger to her health by exposure to EMF/radio frequency radiation (from SMART or similar meters) will make her difficult health situation worse and should be avoided.

I've written a much more detailed letter than this email to the MPSC. You can refer to MPSC Case No. U-17988. If you wish, I would be happy to send the material related to that case which further substantiates my complaint and reasoning for rejecting the installation of a SMART meter (even if it is"turned off"), along with the MPSC's reply in which they seem to consider violation of privacy rights and health risks to be inadequate reasons for opting out of SMART EMF/radio-frequency radiation) meters.

I regret not being able to appear in person before the committee.

Thank you for your consideration and again, I strongly encourage the support of HB4220.

Fred Kummer
37328 Dundee St.
Sterling Heights, MI 48310
</HTML>

Kevin Gawronski

From: Eliisa Seigle <emssds@sbcglobal.net>
Sent: Tuesday, March 7, 2017 6:09 AM
To: Kevin Gawronski
Subject: Analog Choice Bill

We need to PASS the Analog Choice Bill HB 4220!!!!!!
Thank you for making it happen.

God Bless Be happy!
Eliisa M Seigle

Kevin Gawronski

From: blessedtobea blessing <blessedtobeablessing@gmail.com>
Sent: Tuesday, March 7, 2017 8:27 AM
To: Kevin Gawronski
Subject: RE: Support of HB4220

To: House Energy Committee

Please pass HB4220. Michigan residents need to have a "CHOICE" on what goes on our homes. These "smart meters" have many problems associated with the technology that is in these meters and they never should have been installed on the homes. These meters have been force installed by DTE and never tested as DTE says.

Thank you for passing HB4220.

God Bless,

Jackie Ryan
5573 Gardner St E
Sterling Heights, MI 48310

Kevin Gawronski

From: Lisa Graves <lmgraves@gmail.com>
Sent: Tuesday, March 7, 2017 9:47 AM
To: Kevin Gawronski
Subject: Analog Choice Bill

Dear Representative Gawronski,

I'm writing to urge you and your committee to facilitate the passage of HB4220 in 2017.

Like many others, I experience severe ringing in my ears, joint aches, and insomnia when exposed to so-called "smart" meters. I believe that, although privacy rights and fire safety issues apply here also, the health implications are paramount and need to be considered. I and other MI residents simply want to be able to choose to keep our analog meters, instead of being forced to have digital meters of any kind installed on our homes.

Thank you for your time and assistance!

Lisa Graves
315 Glenhaven NW
Grand Rapids MI 49504
(75th District)

Kevin Gawronski

From: cometwatcher@lycos.com
Sent: Tuesday, March 7, 2017 10:14 AM
To: Kevin Gawronski
Subject: HB 4220 The Analog Meter Choice Bill

Mar. 07, 2017

Kevin Gawronski, House Energy Committee Clerk

Re: HB 4220 The Analog Meter Choice Bill

Greetings Mr. Gawronski

Thank you for allowing me submit this information to the House Energy Committee.

As the reasoning for Smart Meter acceptance is proving less beneficial over time, I have noticed a large gap in logical consideration, which is "Data Hacking." (see FBI below)

So called "Smart" Meters can be hacked by computers, Analog meters are immune.

Computer hacking a smart meter can produce a "energy usage pattern," over time, and indicate when you are not home, exposing an opportune window for intruders.

A hacker can cut power and disable security system components in a home or business.

Such incidents will only become more common with the proliferation of smart meters and advancements in computer software and hardware.

It never fails, does it.

I am asking all to please support HB 4220 The Analog Choice Bill.

Thank you for your good work and support.

NOTE: In 2009, the **Federal Bureau of Investigation** investigated widespread incidents of power thefts in Puerto Rico believed to be related to smart meter deployment. The perpetrators were said to have hacked into the smart meters using an optical converter device connected to a laptop, allowing smart meters to connect with the computer. The hackers were able to change the settings for recording power consumptions using software available on the Internet after making a connection. This method does not require the removal, alteration or disassembly of the meter.

Robert Hall

13610 Main St.

Bath, MI 48808

(517) 582-9437

Kevin Gawronski

From: Lisa Gustin <gustinlisa@yahoo.com>
Sent: Tuesday, March 7, 2017 11:32 AM
To: Kevin Gawronski
Subject: HB4220

I am asking for your support on HB4200. I feel very strongly that people should be able to make the choice for themselves as there are health and privacy concerns involved. Thank you. Sincerely Lisa Gustin. Shelby Township

Sent from Yahoo Mail on Android

Before the Michigan House Energy Committee
Hearing on HB 4220 - Meter Choice Bill

December 21, 2017

Exhibit to accompany testimony of
David Sheldon*

Testifying For the Bill

The exhibit consists of excerpts from a report of a federal government task force charged with examining the privacy implications of smart meters and smart grid.

* David Sheldon holds an MBA, B.A. in physics and economics, is certified in software engineering and has 20 years experience in software development prior to his retirement.

Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid

The Smart Grid Interoperability Panel–Cyber Security Working Group

August 2010

****

What follows are excerpts from NISTIR 7628, a report of the National Institute of Science and Technology, U.S. Dept of Commerce. The complete report may be found here: https://www.nist.gov/sites/default/files/documents/smartgrid/nistir-7628_total.pdf

****

5.1 What Is Privacy?

There is no one universal, internationally accepted definition of "privacy," it can mean many things to different individuals. At its most basic, privacy can be seen as the right to be left alone.[4] Privacy is not a plainly delineated concept and is not simply the specifications provided within laws and regulations. Furthermore, privacy should not be confused, as it often is, with being the same as confidentiality; and personal information[5] is not the same as confidential information.

Confidential information[6] is information for which access should be limited to only those with a business need to know and that could result in compromise to a system, data, application, or other business function if inappropriately shared.[7]

It is important to understand that privacy considerations with respect to the Smart Grid include examining the rights, values, and interests of *individuals*; it involves the related characteristics, descriptive information and labels, activities, and opinions of individuals, to name just a few applicable considerations.

For example, some have described privacy as consisting of four dimensions:

1. **Privacy of personal information.** This is the most commonly thought-of dimension. Personal information is any information relating to an individual, who can be identified, directly or indirectly, by that information and in particular by reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural, locational or social identity. Privacy of personal information involves the right to control when, where, how, to whom, and to what extent an individual shares their own personal information, as well as the

right to access personal information given to others, to correct it, and to ensure it is safeguarded and disposed of appropriately.

2. **Privacy of the person.** This is the right to control the integrity of one's own body. It covers such things as physical requirements, health problems, and required medical devices.
3. **Privacy of personal behavior**. This is the right of individuals to keep any knowledge of their activities, and their choices, from being shared with others.
4. **Privacy of personal communications**. This is the right to communicate without undue surveillance, monitoring, or censorship.

Most Smart Grid entities directly address the first dimension, because most data protection laws and regulations cover privacy of personal information. However, the other three dimensions are important privacy considerations as well; thus dimensions 2, 3, and 4 should also be considered in the Smart Grid context because new types of energy use data can be created and communicated. For instance, we can recognize unique electric signatures for consumer electronics and appliances and develop detailed, time-stamped activity reports within personal dwellings. Charging station information can detail whereabouts of an EV. This data did not exist before the application of Smart Grid technologies.

5.3.5 General Invasion of Privacy Concerns with Smart Grid Data

Two aspects of the Smart Grid may raise new legal privacy issues. First, the Smart Grid significantly expands the amount of data available in more granular form as related to the nature and frequency of energy consumption and creation, thereby opening up more opportunities for general invasion of privacy. Suddenly a much more detailed picture can be obtained about activities within a given dwelling, building, or other property, and the time patterns associated with those activities make it possible to detect the presence of specific types of energy consumption or generation equipment. Granular energy data may even indicate the number of individuals in a dwelling unit, which could also reveal when the dwelling is empty or is occupied by more people than usual. The public sharing of information about a specific location's energy use is also a distinct possibility. For example, a homeowner rigged his washing machine to announce the completion of its cycle via his social networking page so that the machine need not be monitored directly.[17] This raises the concern that persons other than those living within the dwelling but having access to energy data could likewise automate public sharing of private events without the dwellers' consent—a general invasion of privacy.

The concern exists that the prevalence of granular energy data could lead to actions on the part of law enforcement —possibly unlawful in themselves—and lead to an invasion of privacy, such as remote surveillance or inference of individual behavior within dwellings, that could be potentially harmful to the dwelling's residents. Law enforcement agencies have already used monthly electricity consumption data in criminal investigations. For example, in *Kyllo v. United States*,[18] the government relied on monthly electrical utility records to develop its case against a suspected marijuana grower.[19] Government agents issued a subpoena to the suspect's utility to obtain energy usage records and then used a utility-prepared "guide for

estimating appropriate power usage relative to square footage, type of heating and accessories, and the number of people who occupy the residence" to show that the suspect's power usage was "excessive" and thus "consistent with" a marijuana-growing operation.

As Smart Grid technologies collect more detailed data about households, one concern identified by the privacy group as well as expressed by multiple published comments is that law enforcement officials may become more interested in accessing that data for investigations or to develop cases. For instance, agencies may want to establish or confirm presence at an address at a certain critical time or even establish certain activities within the home —information that may be readily gleaned from Smart Grid data.

However, the Supreme Court in *Kyllo* clearly reaffirmed the heightened Fourth Amendment privacy interest in the home and noted this interest is not outweighed by technology that allows government agents to "see" into the suspect's home without actually entering the premises.[21] The Court stated, "We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical intrusion into a constitutionally protected area, constitutes a search" and is "presumptively unreasonable without a warrant . ...

Second, unlike the traditional energy grid, the Smart Grid may be viewed as carrying private and/or confidential electronic communications between utilities and end-users, possibly between utilities and third parties[23], and between end-users and third parties. Current law both protects private electronic communications and permits government access to real-time and stored communications, as well as communications transactional records, using a variety of legal processes.[24] Moreover, under the Communications Assistance for Law Enforcement Act (CALEA), telecommunications carriers and equipment manufacturers are required to design their systems to enable lawful access to communications.[25] The granular Smart Grid data may also have parallels to call detail records collected by telecommunications providers. It is unclear if laws that regulate government access to communications will also apply to the Smart Grid.

In short, the innovative technologies of the Smart Grid pose new legal issues for privacy of the home, as well as any type of property location that has traditionally received strong Fourth Amendment protection. As Justice Scalia wrote in *Kyllo*: "The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."

5.3.6 Smart Grid Introduces a New Privacy Dimension

The ability to access, analyze, and respond to much more precise and detailed data from all levels of the electric grid is critical to the major benefits of the Smart Grid—and it is also a significant concern from a privacy viewpoint, especially when this data and data extrapolations are associated with individual consumers or locations. Some articles in the public media have raised serious concerns[27] about the type and amount of billing, usage, appliance, and other related information flowing throughout the various components of the Smart Grid.

There are also concerns across multiple industries about data aggregation of "anonymized" data.[28] For example, in other situations, associating pieces of anonymized data with other publicly available non-anonymous data sets has been shown by various studies to actually reveal specific individuals.[29] Figure 5-1 illustrates how frequent meter readings may provide a detailed timeline of activities occurring inside a metered location and could also lead to knowledge about specific equipment usage or other internal home/business processes.

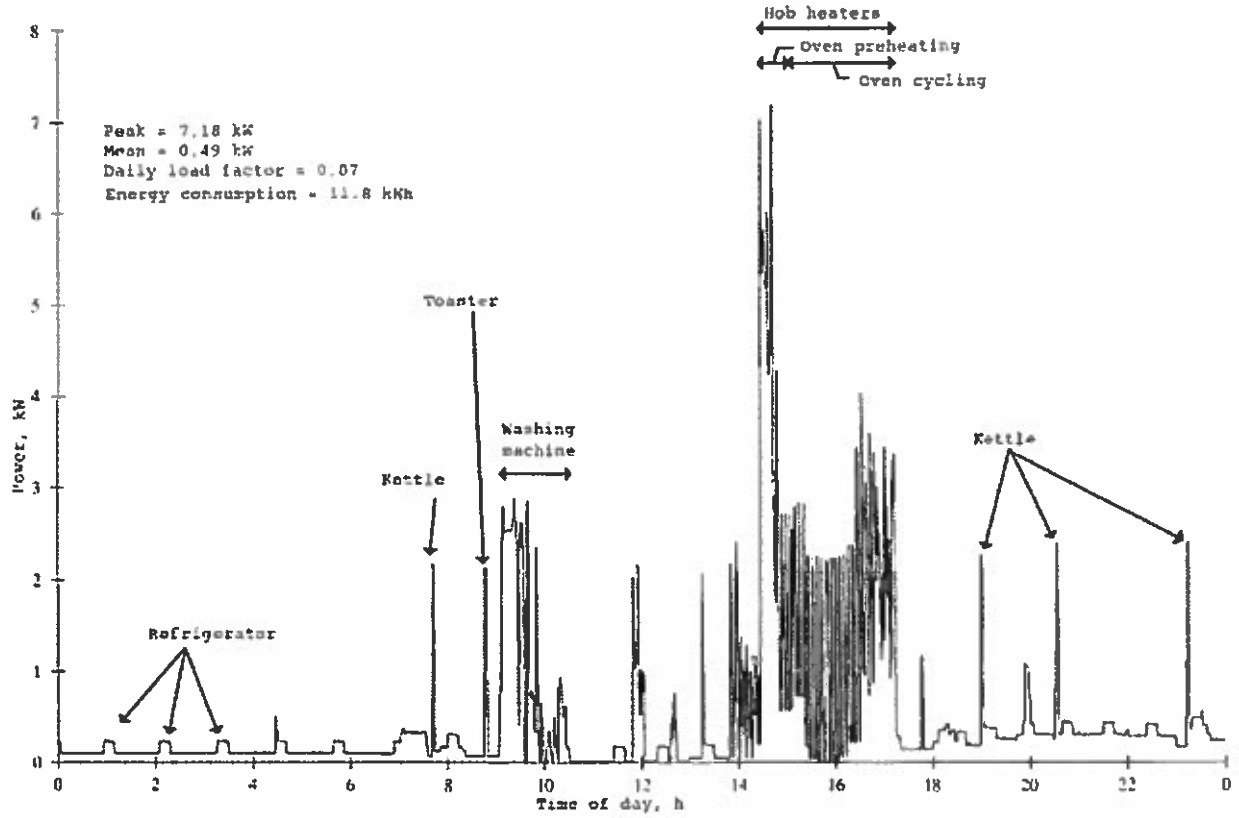

Figure 5-1 Power Usage to Personal Activity Mapping

Smart meter data raises potential surveillance possibilities posing physical, financial, and reputational risks. Because smart meters collect energy usage data at much shorter time intervals than in the past (in 15-minute or sub-15-minute intervals rather than once a month), the information they collect can reveal much more detailed information about the activities within a dwelling or other premises than was available in the past. This is because smart meter data provides information about the usage patterns for individual appliances—which in turn can reveal detailed information about activities within a premise through the use of nonintrusive appliance load monitoring (NALM) techniques.[31] Using NALM, appliances' energy usageprofiles can be compared to libraries of known patterns and matched to identify individual appliances.[32] For example, research shows that analyzing 15-minute interval aggregate household energy consumption data can by itself pinpoint the use of most major home appliances.[33, 34] The graph shown above (Figure 5-1) depicts NALM results as applied to ahousehold's energy use over a 24-hour period. NALM techniques have many beneficial uses,

including pinpointing loads for purposes of load balancing or increasing energy efficiency.

However, such detailed information about appliance use can also reveal whether a building is occupied or vacant, show residency patterns over time, and reflect intimate details of people's lives and their habits and preferences inside their homes.[35] In 1989, George W. Hart, one of the inventors of NALM, explained the surveillance potential of the technique in an article in IEEE Technology and Society Magazine.[36] As the time intervals between smart meter data collection points decreases, appliance use will be inferable from overall utility usage data and other Smart Grid data with even greater accuracy.

In general, more data, and more detailed data, may be collected, generated, and aggregated through Smart Grid operations than previously collected through monthly meter readings and distribution grid operations. Figure 5-2 presents the NIST conceptual model illustrating how data collection can be expected to proliferate as networked grid components increase. In addition to utilities, new entities may also seek to collect, access, and use smart meter data (e.g., vendors creating applications and services specifically for smart appliances, smart meters, and other building-based solutions). Further, once uniquely identifiable "smart" appliances are in use, they will communicate even more specific information directly to utilities, consumers, and other entities, thus adding to the detailed picture of activity within a premise that NALM can provide.

My name is Jaime Chimner from Cheboygan, Michigan near the Mackinaw Bridge. I am Permanently Disabled.

From 2009 to August 2015 I had a (supposedly non transmitting) digital opt out meter on my house and I was unaware of it. On August 2015 my husband Joe cut the main breaker on the house. Why? You may ask. My health, and his, had deteriorated soon after moving into his home in 2009. I went from a cane to a walker to a wheelchair and homebound by 2015. I was paralyzed from the waist down most days and in such severe sharp pain through out my body continuously at its worse from 2013 to August 20, 2015. I wanted to die. That next morning after he shut off the breaker I could walk! My pain level was greatly reduced and I was laughing! My husband,and friend and Doctors were in shock.

4 of my Doctors wrote letters stating I needed an analog meter on my house for my health or I could die. On August 20, 2015 Joe immediately ordered an Analog meter and he put it on the house August 26, 2015. I could finally live in my house without a headache, buzzing in my head and body, muscle spasms, jerk movements, blindness, anxious. I have muscle damage throughout my body now and I am Electricalmagnetic Hypersensitive now as well as other sensitivities. That digital meter intensified what medical issues I may have had and added others. No one will help us!

Consumers Energy wouldn't work with us. **They cut our power on Sept. 11, 2015 because I refused the digital meter back on my house.** Mr. Dennis McKee from Consumers Energy cut our power at 2 pm sept. 11, 2015. We are going through our second winter without electric and I am permanently disabled. So we could survive we had to take out a loan to get natural gas radiating heaters, batteries so we could recharge for LED strip lighting, a generator we didn't have and the gas for it, how were we going to keep our chickens and ducks warm in the winter.. We couldn't afford that. I have medical devices that need electricity to work. My health has improved 10 fold since that digital meter was taken off our home but I was left with worsened asthma, the need for my breathing machine, my special air cleaners and other machines I need. But we still have no electricity and Consumers has decided we don't exist,,,,unless I take a digital meter on my house.

That digital meter was from 2006, the first year they put in the switch mode power supply. That is the main problem with the smart meters and digital meters. The analog meter has surge arrresters and digital meters don't and the smart meters aren't UL approved or ANY independent approval. It is harmful to your helath, I AM THE EVIDENCE as are many more people here. But no one will help us.

Part of the solution is to hardwire computers, hardwire your phone, DTE opted us out of the new gas meter and we didn't even have to ask, ATT hardwired our phone no problem, the local water company opted us out of the smart water meter, they didn't want to subject us to that also. Now where is the problem with Consumers?? As so many people tell us-they can't believe we still don't have electricity and what was Consumers problem? I ask myself that daily.

We DESPERATELY need METER CHOICE in order for any chance of electricity with a mechanical analog meter. Please support this bill.

I am so grateful to have most of my life back but we feel punished. Joe wanted to find the reason for my decline and he was afraid I couldn't hold on any longer. It seems a man gets punished for saving his wife's life.

Please help us.

Respectfully

Jaime Chimner

2/20/2017

Arlene P McGuire
12830 Cherry
Southgate, MI 48195
Mailing Address: P O Box 134 - Allen Park, MI 48101
email: iamcguire444@yahoo.com
cell: 734-637-4744

March 7, 2017

To: Committee on Energy and Technology - Lansing, MI

RE: HB4220 - For the Record

I was forced to accept a Smart Meter because DTE shut off my electricity for 14 days and I had no other option "if I wanted to have electricity" as DTE told me they had to install this Smart Meter. It was not long after, with numerous telephone requests I made to DTE about an electrical issue due to my lights dimming frequently, they finally came out and decided to replace this new Smart Meter. Within days of DTE's visit, I had a fire in my meter box due to "arcing" which was fully documented with pictures by the Master Electrician I engaged to take care of the fire damage and replace the receptacle box and wiring. The Master Electrician indicated I needed to have DTE replace the line from the pole to the house as it was cracked and frayed; however, it took months and many more phone calls to get them to even "assess" the situation. Finally all the electricity on one side of the house went out and DTE finally came out and found they needed to replace the line from the pole to the house - surprise? They are SLOW to respond, inept in repairing, but good at collecting my monthly payment.

I since learned that "arcing" is due to four primary factors (but there are many more):

1) remote disconnect
2) bad installation
3) installing under load
4) thinner blades

There is an exceptional YouTube video explaining about arcing as well as Smart Meter fires in North America and the extreme dangers of these devices. In fact, one of the fires in the video just happened to be a Michigan resident. Please take time to visit:

Smart Meter Fires (2016): Burning meters, burning questions, shocking answers: *https://www.youtube.com/watch?v=7MfiNYzdi24*

As if a single fire isn't bad enough, there are areas in the U.S. where there have been reported electrical outages and 500 smart meters exploded in a community; not only did the homes have damages from the fires, but many had appliances damaged as well. This incident occurred in Stockton, California. Please see the referenced article attached regarding this situation. And you will find much supporting evidence on the internet as well.

In addition, now we are looking at issues with insurance coverage for Smart Meter fires as well. It seems that if the homeowner's Smart Meter box is not up-to-date, the homeowner must pay the cost for the upgrade which amounts to about $800-$1200. If the upgrade is not done, their insurance company could deny any claim and the Smart Meter fire would be the sole responsibility of the homeowner. Please see my enclosed document entitled, "Insurance Exclusions based on EMF Risks".

An analog meter NEVER would have caught fire. They are safe, well-constructed and have a long life. I want mine BACK.

I also want to state that my bill went up about 30% from my previous Senior Citizen monthly rate - from $162 per month to $232 per month - and I am rarely at home, so I find it hard to understand WHY it would increase that much. Faulty meter? System tampering? Who knows? But this is just the start of the increases we'll be seeing because the life of the Smart Meter is so short.

In closing, I have felt uneasy ever since the Smart Meter was put on my house. I could have died in this fire, lost my home. It is chilling to consider. What's worse is the horrific way DTE treated me while trying to resolve my electrical issues.

I want to have a CHOICE regarding something so dangerous - I want my analog meter back.

Sincerely,

Arlene P. McGuire

Arlene P. McGuire

Attachments (3)

'Smart' meter fire situation continues to escalate (KSHB-TV, Kansas City)

August 30, 2016

by Take Back Your Power (www.takebackyourpower.net)

Smart Meter Fires (2016): Burning meters, burning questions, shocking answers: *IMPORTANT YOUTUBE: https://www.youtube.com/watch?v=7MfiNYzdi24*

By Andy Alcock, KSHB-TV | See original article
https://youtu.be/yV_cHlxKoIE

KANSAS CITY, Mo. – Nearly every home and business in the metro have one.

Kansas City Power & Light is at the tail end of a two and a half year project to install more than 700,000 smart meters across the metro.

It's a small part of the billions of dollars utilities have invested in smart meters across the U.S.

But there are serious concerns Waverly Galbreath experienced firsthand. The burn marks are visible on his KCMO home.

A burned-out circuit board is the only remaining part of the smart meter at Galbreath's home where the July fire started.

image: KSHB-TV

Galbreath wasn't at home when it started.

"I got a call from my neighbor and he said my house was on fire. But when I arrived, I found out the meter had exploded," he said.

A KCP&L spokeswoman said the utility is investigating the fire, but she said this type of issue in the metro is very rare.

KCP&L Vice President Chuck Caisley said in a statement to the 41 Action News Investigators, "Out of the more than 700,000 meters KCP&L has installed, we are only aware of a handful of meter malfunctions."

There are multiple smart meter makers and different models.

The company KCP&L uses has had past issues in other places.

Despite few problems in the metro, hundreds of thousands of smart meters have been recalled in the last several years across North America.

And hundreds of fires have broken out in California, Texas, Florida, Nevada, Illinois and across Canada.

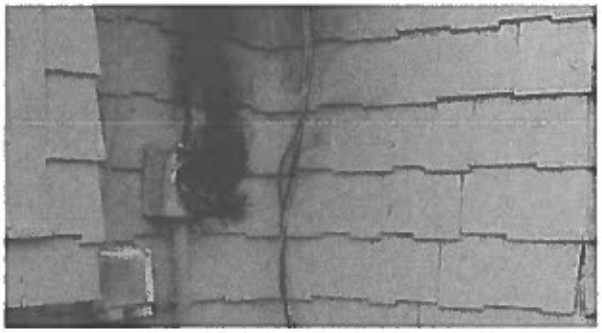

image: Waverly Galbreath

"It really is a very dangerous issue and should be treated as a real unprecedented emergency in your area," said Canadian electrician Professor Curtis Bennett.

Bennett is in an ongoing Canadian legal battle over smart meters.

Bennett sent the 41 Action News Investigators thermal images showing a dangerous smart meter connection running too hot and a normal one.

"Now you've got this plastic piece of junk on their property and that's actually what's burning inside that meter base with the wires," he said.

But Caisley said KCP&L has had a total of six problems out of more than 700,000 meters.

He said the utility has returned a couple meters which have overheated to its supplier.

California insurance adjuster Norman Lambe currently has seven open smart meter fire claims on his desk.

Of the dozens of smart meter fires he's investigated, he said overheating is the major issue.

"They are sparking, they are manufacturing too much heat," he said. "In any given situation when you have too much heat and you have material to burn, meaning unfortunately wiring in the individual's home or business, you're going to have a fire."

America's utilities are spending billions of dollars to install smart meters.

The old ones with the dials, called analog meters, only recorded electricity usage, requiring a meter reader to get the information.

Smart meters transmit your usage information to the power company.

Lambe said those transmissions can cause overheating.

Canadian Brian Thiesen has spent hundreds of hours over five years researching smart meters. He produced a video about smart meter fires. **https://www.youtube.com/watch?v=7MfiNYzdi24**

"These fires are going to continue to happen because again, the basic laws of electricity are being violated," Thiesen said.

But KCP&L's statement said, "At this point, we have found nothing that leads us to believe there is a problem or safety issue with the new meters."

Galbreath has a different take.

He was without power for over a month after his home's smart meter fire. He said he's lucky the wood-shingled home didn't go up in flames.

When asked if other metro residents should be concerned about smart meters he said, "I think so, I really do."

KCP&L said the type of smart meters they're using have not been recalled.

The utility's statement also said the vast majority of house fires are caused by factors other than meters like outdated and overloaded wiring.

Bennett told the 41 Action News Investigators smart meter connections to old bases and faulty wiring are a serious part of the fire problem.

A spokesman for the Board of Public Utilities, BPU, said that utility has installed 70,000 smart meters in Wyandotte County.

BPU spokesman David Mehlhaff said there have been no reports of smart meter fires there.

To check on your own meter, Lambe said the best way is to feel your meter at the end of the day when it's cool outside.

He said if it's hot to the touch, call your utility company.

SMART METER FIRES: Fatalities & Liability

- ***Another 100 smart meters simultaneously explode (Capitola, CA – May 2015)***
- ***Hundreds of smart meters simultaneously explode (Stockton, CA – April 2015)***
- ***Smart meter fire kills 74-year old man in Dallas, Texas (February 2015)***
- ***Man dies in "smart" meter fire (Vacaville, CA – July 2013)***
- ***Fatal fire, smart meter suspected: "Be very aware, very vigilant" says Fire Chief (Reno, NV – Sept 2014)***
- ***Couple escapes house fire, dogs killed: smart meter blamed (Detroit, MI – October 2014)***
- ***ALL 1.2M Elster "smart" meters to be replaced in Arizona (November 2015)***
- ***SaskPower to replace 105,000 faulty "smart" meters (Saskatchewan, CAN – July 2014)***
- ***SaskPower CEO resigns following investigation into smart meter "catastrophe" (October 2014)***
- ***PGE to replace 70,000 faulty "smart" meters (Portland, OR – July 2014)***
- ***Lakeland Electric to replace over 10,000 faulty "smart" meters (Lakeland, FL – August 2014)***
- ***Are tens of thousands of defective "smart" meters being stealthily replaced in Arizona? (Sept 2014)***
- ***PECO replaces 186,000 faulty "smart" meters (Philadelphia, PA – October 2012)***
- ***News & articles on fires – Take Back Your Power***
- ***Archive of hundreds of documented "smart" meter fires – EMF Safety Network***

SEE ALSO:

Smart Meter Fires: Burning meters, burning questions, shocking answers (video): https://takebackyourpower.net/smart-meter-fires-2016-video/

About the Author

Take Back Your Power is revelatory documentary investigating so-called "smart" meters, which governments and utilities are deploying under a guise of *climate action* — without homeowners' consent or knowledge of the facts. What's at stake is in-home surveillance, systemic over-billing, home fires, health & environmental harm, extortion and hacking vulnerability. What you'll discover will shock, unsettle and ultimately empower you. www.takebackyourpower.net

Insurance exclusions based on EMF risks

Now some major players in the insurance world are taking their own stance against the risks being posed by exposure wireless technology including "smart meters". A global insurer, Lloyd's of London, known for taking on risky policies has put in a major exclusion clause for all policy holders, to exclude coverage related to exposure to wireless devices as of February 7, 2015.

Lloyd's of London is one of the largest insurers in the world and often leads the way in protection, taking on risks that no one else will. The Electromagnetic Fields Exclusion (Exclusion 32) is a General Insurance Exclusion and is applied across the market as standard. The purpose of the exclusion is to exclude cover for illnesses caused by continuous long-term non-ionising radiation exposure i.e. through mobile phone usage.

This means that the Province (that is we, the taxpayer) will be held liable for claims from teachers and parents of children suffering biological effects from wifi in schools, from homeowners exposed to RF from mandated smart meters on homes, and from employees forced to use cell phones or exposed to wifi at work. Lawsuits in other countries have resulted in huge payments already, and it is only a matter of time before similar lawsuits are filed and won in Canada.

Potentially those who allow such devices, after having been fully informed about the dangers, could be held liable for negligence, and directors' insurance may not provide financial protection. Directors' insurance applies when people are performing their duties "in good faith". It is hard to argue they are acting "in good faith" after having been warned by true scientific experts and by a well-respected insurer. (Excerpt from letter by Sharon Noble Director, Coalition to Stop Smart Meters in British Columbia Victoria, British Columbia, Canada)

Lloyd's exclusion is basically on all of their liability insurance policies. Without reinsurance coverage all insurance policies will exclude coverage of health damaging radiation. If suits for cancer and other associated health issues occur from wireless radiation exposure there would be a catastrophic influx of claims. This is a standard liability insurance response to risk exposure from a global and universal health danger. Perhaps this could be a repeat to issues like asbestos, chemical hazards in building materials and other types of toxic exposure.

Policy exclusions very specific

From the Lloyd's of London policy: "Exclusions (starting on Page 6 of policy, Page 7 of pdf). We will not:

a) make any payment on your behalf for any claim, or
b) incur any costs and expenses, or
c) reimburse you for any loss, damage, legal expenses, fees or costs sustained by you, or
d) pay any medical expenses:

32. Electromagnetic fields (General Insurance Exclusions - Page 7 of policy): directly or indirectly arising out of, resulting from or contributed to by electromagnetic fields, electromagnetic radiation, electromagnetism, radio waves or noise."

So what does the insurance industry know that the rest of the world has not yet come to terms with?

Sources:

http://www.activistpost.com
In Pennsylvania, House Bills 393, 394, 395, 396, and Senate Bills 816, 817, 818

https://www.stopsmartmetersinpa.com
http://smartmeterharm.org
http://thephaser.com
http://www.citizensforsafetechnology.org
http://citizensforsafetechnolog
http://ehtrust.org

Utility-issued 'smart' meters explode on 5,000 homes after truck rams utility pole

Learn more: http://www.naturalnews.com/049518_smart_meters_EMF_pollution_utilities.html#ixzz3noVwPepU

(NaturalNews) Thousands of California residents were left without power recently after their so-called "smart" meters exploded due to an unexpected power surge. According to *CBS Sacramento*, more than 5,000 homes in the Stockton area were left with blackened, charred, and completely destroyed smart meters after a dump truck crashed into a nearby utility pole, pulling the static line down onto the distribution line.

When the two lines intersect, stated PG&E spokeswoman Brandi Ehlers to the media, the resultant surge causes a major overload to the system. And when smart meters are involved, this overload can cause the meters themselves to pop and literally blow up, potentially causing a fire or other property damage not typically caused by traditional analog meters.

"The top lines are considered our freeways," explained Ehlers. "The bottom lines are our distribution lines taking power directly to homes. So when the two collide, they're at different voltages and the higher voltage wins out, causing an overload."